JL

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/934,166	08/20/2001	Ian Rhodes	930.337USW1	8265

32294 7590 03/30/2006

SQUIRE, SANDERS & DEMPSEY L.L.P.
14TH FLOOR
8000 TOWERS CRESCENT
TYSONS CORNER, VA 22182

EXAMINER	
TRUONG, THANHNGA B	
ART UNIT	**PAPER NUMBER**
2135	

DATE MAILED: 03/30/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action Before the Filing of an Appeal Brief	Application No. 09/934,166	Applicant(s) RHODES, IAN	
	Examiner Thanhnga B. Truong	Art Unit 2135	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 14 March 2006 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☒ The period for reply expires 3 months from the mailing date of the final rejection.
   b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☐ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☐ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: _____. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, ~~the proposed amendment(s): a) ☐ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.~~

   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: *None*.
   Claim(s) objected to: *None*.
   Claim(s) rejected: *1-24,26-54,56 and 59*.
   Claim(s) withdrawn from consideration: *None*.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☒ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: See Continuation Sheet.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). _____
13. ☐ Other: _____.

Continuation of 11. does NOT place the application in condition for allowance because: Applicant's arguments filed March 14, 2006 have been fully considered but they are not persuasive.

Applicant argues that:

Jacobson and Boyd do not disclose or suggest first and second networks separated by a relatively secure intermediate network AND a relatively insecure intermediate network (see applicant's remark, page 9, last 3 lines of first paragraph). Applicant further argues that the cited references do not disclose or suggest selectively routing a packet over one of a relatively secure intermediate network AND a relatively insecure intermediate network by a network element triggerable to refer to information held in a storage means (see applicant's remark, page 12, the middle of the page, page 14, first 3 lines of last paragraph, page 17, lines 2-3).

Examiner still disagrees with the applicant and maintains that:

First of all, the applicant's arguments and the language cites in claims 1, 27 and 37 are not the same. These claims recite the limitation "over said relatively insecure intermediate network OR said relatively secure intermediate network" that has been amended by the applicant in the Amendment filed on September 23, 2005 to overcome the 35 USC 112 2nd paragraph rejection that the office mailed on June 28, 2005 . Applicant is ignoring the change and repeated again here in the above argument using both insecure and secure intermediate networks, in which the arguments do not support by the instant specification. The applicant's specification discloses "the intermediate communication route can either be secure or insecure" (see page 1, lines 36-37 of specification). The term "and" is indefinite because the specification does not clearly redefine the term. Thus, applicant uses terminology inconsistent with the accepted meaning through out the remarks. In other words, the above argument's limitation does not even support by the specification to rescue applicant's position.

Secondly, Jacobson does teach the claimed subject matter. In fact, Jacobson teaches a network local security bridge and corresponding method for bridging a first side of a network and a second side of the network. The first side includes local secure zone host devices within a local secure zone established by the network local security bridge. The second side includes remote secure zone host devices within remote secure zones established by network remote security bridges (see Jacobson's abstract). Besides, data encryption and decryption for secure communication between hosts in a network has existed for many years. In these types of networks (i.e. many networks, more than one networks), each host device is burdened with encrypting outgoing data and decrypting incoming data (column 1, lines 7-12 of Jacobson). In addition, Boyle also teaches two private networks (i.e., plurality of networks, more than one networks) as shown in Figure 2 of Boyle's invention (column 4, lines 51-55 of Boyle).

Thus, the combination of teaching between Jacobson and Boyle teaches the claimed subject matter. Referring again to Figures 2 and 4a-4c, the data packet forwarder 211 selects the source key by first identifying from the identification table 230 the IP address of the network remote security bridge that establishes the remote secure zone which contains the remote secure zone host specified by the parsed IP source address. Then, it selects the source key in the key table 232 that corresponds to the network remote security bridge that it just identified. After the source key has been selected, the data packet forwarder calls up the encryptor/decryptor 233 and passes to it the pointer to the received data packet. The encryptor/decryptor in response decrypts the IP data frame of the received data packet with the selected source key using the DES table 234 contained in the library 216 in accordance with known DES encryption/decryption techniques (block 438 of Figure 4b). The encryptor/decryptor then alerts the data packet forwarder that the IP data frame of the received data packet has been decrypted. The data packet forwarder then returns control to the operating system 210, alerts the operating system that the received data packet has been processed and is to be forwarded to the side opposite from where it was received, and also passes to the operating system the pointer to the received data packet (block 408 of Figure 4c) (column 7, lines 54-67 through column 8, lines 1-10 of Jacobson). Although Jacobson does not explicitly point out the distribution and/or routing of security information between the first network and the second network, Boyle teaches referring to Figure 2, a variation is shown employing SNIUs for internetwork connections. A bridge SNIU is used between two private networks (shaded ovals) using the same security labeling semantics but which operate at two different protection levels. The networks may be controlled by a single network security manager SM, or each network can have its own security manager SM. A gateway SNIU is used between two networks using different security labeling semantics, for example, a Type A network may use labels (Top Secret, Secret, Confidential, Unclassified) and a Type B network may use the labels (Most Secret, Secret, Restricted, Confidential, Releasable). A guard SNIU is used to support communications between a private network and a public network. The network security system of the invention is divided into two major functional areas: the Trusted Session Protocol (TSP) hosted by the SNIU, which is responsible for the management of the data path and the passing of data; and the Security Management architecture, consisting principally of the Security Manager (SM), which is responsible for security management of the network (column 4, lines 51-67 through column 5, lines 1-4 of Boyle).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, The combination of teaching between Jacobson and Boyle is sufficient.

Applicant further argues that:

The cited references, Jacobson and Thomas, either alone or in combination do not disclose or suggest selectively routing, over one of the relatively insecure intermediate network and the relatively secure intermediate network..... to information held in a storage means.

Examiner again disagrees with the applicant and still maintains that:

As mentioned above and repeated herein, the applicant's arguments and the language cites in claims 1, 27 and 37 are not

the same. These claims recite the limitation "over said relatively insecure intermediate network OR said relatively secure intermediate network" that has been amended by the applicant in the Amendment filed on September 23, 2005 to overcome the 35 USC 112 2nd paragraph rejection that the office mailed on June 28, 2005 . Applicant is ignoring the change and repeated again here in the above argument using both insecure and secure intermediate networks, in which the arguments do not support by the instant specification. The applicant's specification discloses "the intermediate communication route can either be secure or insecure" (see page 1, lines 36-37 of specification). The term "and" is indefinite because the specification does not clearly redefine the term. Thus, applicant uses terminology inconsistent with the accepted meaning through out the remarks. In other words, the above argument's limitation does not even support by the specification to rescue applicant's position.

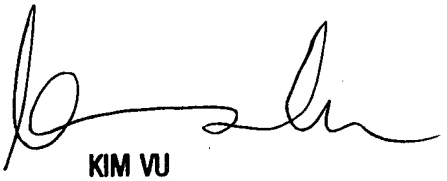
The combination of teaching between Jacobson and Thomas teaches the claimed subject matter. As mentioned above, Jacobson teaches a network local security bridge and corresponding method for bridging a first side of a network and a second side of the network. The first side includes local secure zone host devices within a local secure zone established by the network local security bridge. The second side includes remote secure zone host devices within remote secure zones established by network remote security bridges (see Jacobson's abstract). Although Jacobson does not explicitly discuss accessing point to a subscriber in a visited network by virtue of a roaming agreement between the operator of the visited network and the operator of the subscriber's home network. Thomas teaches allowing a H.323 compliant user to roam to another H.323 compliant network that is recognized by that users home gatekeeper. After arriving at the visited network, the roaming user registers with a visited gatekeeper. The visited gatekeeper authorizes the registration by determining the network of the roaming user and that a roaming agreement exists between the visited and home network (column 6, lines 20-27 of Thomas). Furthermore, Thomas's invention is directed to the method of and apparatus for completing multimedia calls over a packetized data transmission link to a roaming user currently located in a network foreign to the users home network (see Figure 2-4 of Thomas for more details).

In response to applicant's argument that there is no suggestion to combine the references, the examiner recognizes that obviousness can only be established by combining or modifying the teachings of the prior art to produce the claimed invention where there is some teaching, suggestion, or motivation to do so found either in the references themselves or in the knowledge generally available to one of ordinary skill in the art. See In re Fine, 837 F.2d 1071, 5 USPQ2d 1596 (Fed. Cir. 1988)and In re Jones, 958 F.2d 347, 21 USPQ2d 1941 (Fed. Cir. 1992). In this case, The combination of teaching between Jacobson and Thomas is sufficient.

Thus, Jacobson, Boyle, and Thomas do not need to disclose anything over and above the invention as claimed in order to render it unpatentable or anticipate. A recitation of the intended use of the claimed invention must result in a structural difference between the claimed invention and the prior art in order to patentably distinguish the claimed invention from the prior art. If the prior art structure is capable of performing the intended use, then it meets the claimed limitations.

For the above reasons, it is believed that the rejections should be sustained.

In reponse to applicant's withdrawal of the finality, Examiner has carefully reviewed the Office Action mailed on December 14, 2005 and compared with the Office Action mailed on June 28, 2005. The rejection under 35 USC 103 (a) for the two actions were the same. There was a typographical error in using format in the conclusion of the Final Office Action with stated the new ground(s) of rejection. The wrong format was used by the examiner. For this reason, the request to withdraw the finality is denied.



KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100